DETAILED ACTION

1. This Office action is responsive to the following communication: Amendment filed on 24 March 2010.

2. Claims 1-2, 5-9, 12-18, 21-25, 28-34, 37-40, and 43-44 are pending and present for examination. Claims 1, 8, 15, 17, 24, 31, 33, and 39 are in independent form.

Response to Amendment

3. No claims have been amended.

4. No claims have been newly added.

5. No claims have been further cancelled.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claims 1, 2, 5, 6, 8, 9, 12, 13, 15-19, 24, 25, 28, 29, 31-34, 37, 39, 40, 42, and 43** are rejected under 35 U.S.C. 103(a) as being unpatentable over Owen et al (U.S. Patent No. 6,968,349, hereinafter referred to as OWEN), filed on 16 May 2002, published on 20 November 2003, and issued on 22 November 2005, in view of Pond et al (U.S. Patent No. 4,864,616, hereinafter referred to as POND), filed on 15 October 1987, and issued on 5 September 5, 1989, and in further view of Brown et al (USPGPUB 2003/0023850, hereinafter referred to as BROWN), filed on 26 July 2001, and published on 30 January 2003.

8. **As per independent claims 1 and 17,** OWEN, in combination with POND and BROWN, discloses:

A method, comprising:

receiving a second data record to be stored on a single database, wherein the database comprises a first data record {See OWEN, C8:L6-24, wherein this reads over "the minimized data journal entry is read"};

storing the second data record on the database, wherein the second data record is stored consecutive to the first data record {See OWEN, C8:L38-54, wherein this reads over "the validation value comprises a checksum that is computed using both the data in the old record and the metadata for the old record"};

retrieving a first integrity checksum stored with the first data record previous to the second data record {See OWEN, C8:L38-54, wherein this reads over "the validation value comprises a checksum that is computed using both the data in the old record and the metadata for the old record"; and C8:L55-C9:L10, wherein this reads over "[t]he validation value of the preferred embodiments is a value that relates to the state of the record that corresponds to the journal entry just before applying the changes reflected in the journal entry"};

computing a second integrity checksum for the second data record with a cryptographic method using a storage key, the retrieved first integrity checksum and the second data record {See OWEN, C10:L8-27, wherein this reads over "[w]hen the minimized data journal entry is to be applied to the corresponding database record, a validation value for the record is first computed using the same algorithm used to compute the validation value stored in the journal entry"}, wherein the storage key represents an identity of a signing entity authorized to sign data records {See BROWN, Para. 0049, wherein this reads over "[t]he private key further encrypts a checksum determined for the contents log file that is stored with the signature"};

storing the second integrity checksum on the database {See OWEN, C10:L8-27, wherein this reads over "[t]his validation value is then stored as apart of the minimized data journal entry"}; and

configuring the retrieved integrity checksum for a first row of the database to be a generated initialization vector {See POND, C3:L53-62, wherein this reads over "[t]he initialization vector contains bits for indicating the starting bye in each of the key streams used for encryption and decryption. The Checksum is derived by summing the . . . the Initialization Vector and issued to confirm the integrity of the label"} or a digital signature of a signing entity.

While OWEN may fail to expressly disclose a method for configuring a retrieved integrity checksum for a first row of the database to be a generated initialization vector, POND discloses a method wherein an initialization vector is used to derive a checksum. The combination of inventions disclosed in OWEN and POND would disclose a method wherein the integrity checksum for a first row of a database is a generated initialization vector. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by OWEN by combining it with the invention disclosed by POND.

One of ordinary skill in the art would have been motivated to do this modification so that where there is no previous integrity checksum available, the initialization vector may be used to in the computation of a second integrity checksum.

The combination of inventions disclosed in OWEN and BROWN would disclose a method wherein the storage key is a private key used for verification purposes in a public key infrastructure. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by OWEN by combining it with the invention disclosed by BROWN.

One of ordinary skill in the art would have been motivated to do this modification so that the integrity of the signing entity may be verified.

9. **As per dependent claims 2, 18, and 34,** OWEN, in combination with POND and BROWN, discloses:

The method according to claim 8, further comprising:

configuring the storage key to be a secret key of public key infrastructure {See BROWN, Para. 0049, wherein this reads over "[t]he private key further encrypts a checksum determined for the contents log file that is stored with the signature"}.

The combination of inventions disclosed in OWEN and BROWN would disclose a method wherein the storage key is a private key used for verification purposes in a public key infrastructure. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by OWEN by combining it with the invention disclosed by BROWN.

One of ordinary skill in the art would have been motivated to do this modification so that the integrity of the signing entity may be verified.

10. **As per dependent claims 5, 12, 21, 28, 37, and 43,** OWEN, in combination with POND and BROWN, discloses:

The method according to claim 8, wherein the retrieving the first integrity checksum comprises retrieving the first integrity checksum from a memory of a verification entity {See OWEN, C8:L8-24, wherein this reads over "[t]he generated validation value is then compared against the validation value stored in the minimized data journal entry"}.

11. **As per dependent claims 6, 13, 22, and 29,** OWEN, in combination with POND and BROWN, discloses:

The method according to claim 8, further comprising:

storing the second integrity checksum on a memory of a verification entity {See OWEN, C10:L8-27, wherein this reads over "[t]his validation value is then stored as apart of the minimized data journal entry"}.

12. **As per independent claims 8, 15, 24, 31, 33, and 39,** OWEN, in combination with POND and BROWN, discloses:

A method, comprising:

retrieving a second data record to be verified from a single database {See OWEN, C8:L6-24, wherein this reads over "the minimized data journal entry is read"};

retrieving a second integrity checksum of the second data record, wherein the first data record and the second data record are consecutive data records in the database {See OWEN, C8:L38-54, wherein this reads over "[a]nother type of suitable validation value is a cyclic redundancy check (CRC) that provides a unique value that indicates the state of the record before applying the change"; and C10:L8-27, wherein this reads over "[w]hen the minimized data journal entry is to be applied to the corresponding database record, a validation value for the record is first computed using the same algorithm used to compute the validation value stored in the journal entry"};

retrieving a first integrity checksum of the first data record previous to the retrieved second data record {See OWEN, C8:L38-54, wherein this reads over "the validation value comprises a checksum that is computed using both the data in the old record and the metadata for the old record"; and C8:L55-C9:L10, wherein this reads over "[t]he validation value of the preferred embodiments is a value that relates to the state of the record that corresponds to the journal entry just before applying the changes reflected in the journal entry"};

computing a third integrity checksum for the second data record using the retrieved second data record, the first integrity checksum, and a storage key {See OWEN, C10:L8-27, wherein this reads over "[w]hen the minimized data journal entry is to be applied to the corresponding database record, a validation value for the record is first computed using the same algorithm used to compute the validation value stored in the journal entry"}, wherein the storage key represents an identity of a signing entity authorized to sign data records {See BROWN, Para. 0049, wherein this reads over "[t]he private key further encrypts a checksum determined for the contents log file that is stored with the signature"}; and

comparing the second integrity checksum to the third integrity checksum, wherein the second data record is considered authentic when the second integrity checksum and the third integrity checksums are equal {See OWEN, C10:L8-27, wherein this reads over "[i]f the two validation values match, we know with a high level of confidence that the record is in the identical state it was in just before the changes reflected in the journal entry were made"}; and

configuring the retrieved integrity checksum for a first row of the database to be a generated initialization vector {See POND, C3:L53-62, wherein this reads over "[t]he initialization vector contains bits for indicating the starting bye in each of the key streams used for

encryption and decryption. The Checksum is derived by summing the . . . the Initialization Vector and issued to confirm the integrity of the label"} or a digital signature of a signing entity.

While OWEN may fail to expressly disclose a method for configuring a retrieved integrity checksum for a first row of the database to be a generated initialization vector, POND discloses a method wherein an initialization vector is used to derive a checksum. The combination of inventions disclosed in OWEN and POND would disclose a method wherein the integrity checksum for a first row of a database is a generated initialization vector. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by OWEN by combining it with the invention disclosed by POND.

One of ordinary skill in the art would have been motivated to do this modification so that where there is no previous integrity checksum available, the initialization vector may be used to in the computation of a second integrity checksum.

The combination of inventions disclosed in OWEN and BROWN would disclose a method wherein the storage key is a private key used for verification purposes in a public key infrastructure. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by OWEN by combining it with the invention disclosed by BROWN.

One of ordinary skill in the art would have been motivated to do this modification so that the integrity of the signing entity may be verified.

13. **As per dependent claims 9, 25, and 40,** OWEN, in combination with POND and BROWN, discloses:

The method according to claim 8, further comprising:

configuring the storage key to be a public key of public key infrastructure {See BROWN, Para. 0061, wherein this reads over "In particular, to verify the participants in a messaging session, logging controller 62 utilizes a public key for a user to attempt to decrypt the private key and checksum. If a private key matches a public key, then an identity for a user associated with the public and private keys may be verified. Further, logging controller 62 utilizes the public key to decrypt a checksum for the recorded messaging session and then computes a current checksum for the messaging session. If the checksums match, then the integrity of the messaging session may be verified. In addition, methods other than calculating a checksum may be utilized to verify the integrity of the messaging session"}.

The combination of inventions disclosed in OWEN and BROWN would disclose a method wherein the storage key is a public key used for verification purposes in a public key infrastructure. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by OWEN by combining it with the invention disclosed by BROWN.

One of ordinary skill in the art would have been motivated to do this modification so that the integrity of the signing entity may be verified.

14. **As per dependent claims 16 and 32,** OWEN, in combination with POND and BROWN, discloses:

> The system according to claim 15, wherein the signing entity and verification entity apply public key infrastructure {See BROWN, Para. 0061, wherein this reads over "In particular, to verify the participants in a messaging session, logging controller 62 utilizes a public key for a user to attempt to decrypt the private key and checksum. If a private key matches a public key, then an identity for a user associated with the public and private keys may be verified. Further, logging controller 62 utilizes the public key to decrypt a checksum for the recorded messaging session and then computes a current checksum for the messaging session. If the checksums match, then the integrity of the messaging session may be verified. In addition, methods other than calculating a checksum may be utilized to verify the integrity of the messaging session"} for calculating and verifying the one of the first integrity checksum and the second integrity checksum .

The combination of inventions disclosed in OWEN and BROWN would disclose a method wherein the storage key is a public key used for verification purposes in a public key infrastructure. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by OWEN by combining it with the invention disclosed by BROWN.

One of ordinary skill in the art would have been motivated to do this modification so that the integrity of the signing entity may be verified.

15. **Claims 7, 14, 23, 30, 38, and 44** are rejected under 35 U.S.C. 103(a) as being unpatentable over OWEN, in view of POND, and in further view of Cain (U.S. Patent No. 6,557,044, hereinafter referred to as CAIN), filed on 1 June 1999, and issued on 29 April 2003.

16. **As per dependent claims 7, 14, 23, 30, 38, and 44,** OWEN, in combination with POND and CAIN discloses:

> The method according to claim 8, further comprising:

configuring the integrity checksums to comprise a running sequence number {See CAIN, c2:l64-67, wherein this reads over "incremental checksumming may be utilized. Initially, the checksum for all routes in a set is computed by determining the checksum for all sequence numbers"}.

Response to Arguments

17. Applicant's arguments filed 13 November 2009 have been fully considered but they are not persuasive.

a. Claim Rejections under 35 U.S.C. 103

Applicant asserts the argument that Owen fails to disclose the feature of computing a checksum with a cryptographic method from a second data record, a checksum from a previous data record, and a storage key. See Amendment, page 13. The Examiner respectfully disagrees.

It is noted that Owen discloses a method for validating database records via a validation value. Owen specifically discloses that the validation value "comprises a checksum that is computed using both the data in the old record and the metadata for the old record." See col. 8, lines 44-50. The claimed invention recites a method wherein the second integrity checksum is computed using (1) a storage key, (2) a retrieved first integrity checksum, and (3) a second data record. Owen, in combination with Pond and Brown, would disclose the method for computing a second integrity checksum in that Owen discloses a validation value (i.e. a second integrity checksum) that is calculated using a checksum of an old record (i.e. a retrieved first integrity checksum). Owen further discloses that the checksum is computed "using both the data in the old record and the metadata for the old record" and would appropriately read upon the claimed "second data record" of the present invention. As for the computation of a second integrity checksum using a storage key which "represents an identity of a signing entity authorized to sign data records," Brown discloses a system wherein a private key is used to encrypt a checksum.

Accordingly, the combination of Owen, Brown, and Pond would indeed read upon a method wherein the second integrity checksum is computed using (1) a storage key, (2) a retrieved first integrity checksum, and (3) a second data record.

Accordingly, the rejections under 35 U.S.C. 103 are sustained.

Conclusion

18. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to PAUL KIM whose telephone number is (571)272-2737. The examiner can normally be reached on M-F, 9am - 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tony Mahmoudi can be reached on (571) 272-4078. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tony Mahmoudi/
Supervisory Patent Examiner, Art Unit 2169

Paul Kim
Examiner, Art Unit 2169

/pk/